ABSTRACT

To implement an operation in Jacobian with improved computation complexity, the sum is computed of a divisor D_1=g.c.d. $(a_1(x),y-b_1(x))$ and a divisor D_2=g.c.d. $(a_2(x),y-b_2(x))$ on Jacobian of a hyperelliptic curve $y^2+y=f(x)$ defined over $GF(2^n)$ by: storing $a_1(x)$, $a_2(x)$, $b_1(x)$ and $b_2(x)$; and calculating $q(x)=s_1(b_1(x)+b_2(x))$ mod $a_2(x)$ by using $s_1(x)$ in $s_1(x)a_1(x)+s_2(x)a_2(x)=1$ in case of $GCD(a_1(x),a_2(x))=1$ where GCD denotes a greatest common polynomial. Thus, a new function q(x) is provided so as to reduce the entire computational complexity and the hardware size. Moreover, in the case of $D_1=D_2$, $a_1(x)$ and $b_1(x)$ is stored; and $q(x)=Q(b_1^2(x)+f(x)$ mod $a_1^2(x)$, $a_1(x))$ where Q(A,B) is a quotient of A/B is calculated.